



**UNITED STATES DEPARTMENT OF COMMERCE**  
**National Institute of Standards and Technology**  
Gaithersburg, Maryland 20899-0001

AUG 09 2019

Mr. Steve Weis  
MuckRock News  
DEPT MR 78756  
411A Highland Ave  
Somerville, MA 02144-2516

Dear Mr. Weis:

This acknowledges receipt of your August 9, 2019, Freedom of Information Act (FOIA) request to the National Institute of Standards and Technology (NIST) in which you requested:

Any documents related to the choice of elliptic curves over prime fields for ECC key agreement that first appeared in FIPS 186-4 Appendix D, sections D.1.2.1-D.1.2.5 (<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>). For example, any information to the choice of D.1.2.3: P-256: SEED = c49d3608 86e70493 6a6678e1 139d26b7 819f7e90.

This document has been superseded by NIST 800-56A (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf>). Please return any email, memorandum, presentations, reports, articles, research papers, justifying the choice of initialization parameters for the following standards: P-224 (also known as secp224r1), P-256 (secp256r1), P-384 (secp384r1), P-521 (secp521r1) Dr. Jerry (or Gerald) Solinas from the NSA may have been involved in the parameter selection.

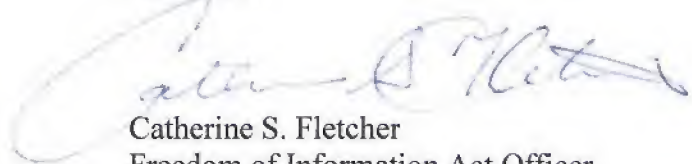
Your request was received at the FOIA Control Desk on August 9, 2019 and was assigned FOIA Log #DOC-NIST-2019-001948.

FOIA allows agencies twenty working days to make a determination on the request. However, it may not always be possible to provide the documents within this time period. In some cases, we may take an extension and will advise you. Please be advised that your request may be subject to fees for search, review, and reproduction costs. Should this be the case, you will be given an estimate of the costs. Fee estimates are developed in good faith and are based on our reasonable judgment. However, due to the unique nature of each request and complexity of documents involved, actual costs to search and review the material may vary from the original estimate.

**NIST**

Maureen O'Reilly, Management Analyst of my office, is the contact point for processing your request. If you have any questions regarding your pending FOIA request, she may be reached by email at [foia@nist.gov](mailto:foia@nist.gov) or by phone (301) 975-3189.

Sincerely,

A handwritten signature in blue ink, appearing to read "Catherine S. Fletcher", is written over a faint, circular official stamp.

Catherine S. Fletcher  
Freedom of Information Act Officer